UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,967	01/30/2001	Mehdi-Laurent Akkar	AKKAR	2638

1444 7590 07/20/2004

BROWDY AND NEIMARK, P.L.L.C.
624 NINTH STREET, NW
SUITE 300
WASHINGTON, DC 20001-5303

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	4

DATE MAILED: 07/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/771,967	AKKAR ET AL.
	Examiner	Art Unit
	Zachary A Davis	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A preliminary amendment was received on 30 January 2001. Claims 1-13 are pending in the present application.

Specification

2. The disclosure is objected to because of the following informalities:

The sections of the specification are not labeled. While the specification does include the required sections of Background, Brief Summary, Brief Description of Drawings, and Detailed Description, each section must be labeled with a section heading. See MPEP § 608.01(a).

The specification appears to contain minor typographical errors. For example, on page 3, line 28, it is assumed that the word "bite" is intended to read as either "bit" or "byte". Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Appropriate correction is required.

Claim Objections

3. Claims 4-5, 8-9, and 12 are objected to because of the following informalities:

The words "one of" in line 1 of each of the above-mentioned claims should be deleted to put the claims in proper dependent form.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1-13 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed to a method of generating a cryptographic protocol; however, the method does not appear to be tangibly embodied in a computer or computer-readable medium. The method appears solely to include abstract ideas that could be used to generate a protocol, and the language of the claim raises a question as to whether these abstract ideas are tied to a technological art, environment, or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

6. To expedite a complete examination of the instant application, the claims rejected under 35 U.S.C. 101 above are further rejected as set forth below in anticipation of applicant amending these claims to place them with in the statutory classes of invention.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1-13 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 is directed to a method of generating a cryptographic protocol. However, there are no method steps recited that clearly describe how such a protocol is generated. This renders the claim indefinite.

Further, Claims 2-5 do not clearly further limit the method of Claim 1, in that it is not clear how the operations recited in Claims 2-5 are to be used in the process of generating a cryptographic protocol.

In reference to Claims 7 and 8, lines 1-2 of each claim read "characterized in that consists in using". This phrase is generally unclear and renders the claim indefinite.

Further in reference to Claim 7, the claim recites the limitation "it" in line 4. It is unclear what the antecedent of "it" is, which renders the claim indefinite. Similarly, further in reference to Claim 8, the claim recites the limitation "it" in line 3, which renders the claim indefinite.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Kocher et al, US Patent 6278783.

In reference to Claim 1, Kocher discloses a cryptographic protocol in which a chain of operations is carried out (Figures 1 and 2; column 1, line 66-column 2, line 24) and in which operations in the chain can be chosen depending on a random decision (column 9, lines 1-13).

In reference to Claims 2-5, Kocher further discloses that XOR operations, permutation operations, indexed access to a table, and operations that are stable with respect to XOR can be used as operations in the chain (column 2, line 44-column 3, line 9, especially column 2, lines 44-45).

In reference to Claim 6, Kocher further discloses that operations that transfer data between memory locations may be performed (column 8, lines 45-57).

In reference to Claim 7, Kocher further discloses that new operations are determined based on a random parameter (column 9, lines 7-13, 30-48, and 62-64) and a counter is updated (column 9, lines 25-27).

In reference to Claim 8, Kocher further discloses that new operations are determined based on a random parameter (column 9, lines 7-13, 30-48, and 62-64) and intermediate responses are transmitted (see column 2, lines 17-19).

In reference to Claim 9, Kocher further discloses two chains of operations (column 6, lines 28-38 and 64-67).

In reference to Claim 10, Kocher further discloses comparing a counter against a threshold value and altering operation based on the comparison (column 9, lines 25-30).

In reference to Claim 11, Kocher further discloses performing operations byte by byte (see column 5, lines 20-27).

In reference to Claim 12, Kocher further discloses performing operations bit by bit (see column 2, line 45; also column 10, lines 51-60).

In reference to Claim 13, Kocher further discloses that the order of execution of operations can be permuted (column 10, lines 51-55).

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Leppek, US Patent 5933501, discloses an encryption scheme using a sequence of differing encryption operations.

b. Matyas, Jr., et al, US Patent 6301362, discloses an encryption method including multiple chains of operations.

c. Patarin et al, US Patent 6658269, discloses a cryptographic process for smart cards in which calculations are divided into parallel processes and the intermediate results of the parallel processes are reconstructed to form an end result.

d. Jahnich et al, US Patent 6725374, discloses an encryption program for a smart card including permuting the order in which subprograms of the program are executed.

e. Schneier, *Applied Cryptography*, discusses the operation and cryptanalysis of DES.

f. Messerges, *Investigations of Power Analysis Attacks on Smartcards*, discusses the need to defend cryptographic methods from power analysis attacks when cryptanalyzing and protecting an encryption algorithm.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (703) 305-8902. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137